*****PUBLIC VERSION*****

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
Alexandria Division

UNITED STATES OF AMERICA, Plaintiff, v. ZACKARY ELLIS SANDERS, Defendant.	Case No. 1:20-cr-00143 The Honorable Judge Ellis Hearing: Sept. 11, 2020

MR. ZACKARY ELLIS SANDERS'S MOTION TO SUPPRESS AND FOR RECONSIDERATION OF HIS MOTION TO COMPEL DISCOVERY

Jonathan Jeffress (#42884)
Emily Voshell (#92997)
Jade Chong-Smith (admitted *pro hac vice*)
KaiserDillon PLLC
1099 14th Street. NW
8th Floor West
Washington, D.C. 20005
Telephone: (202) 683-6150
Facsimile: (202) 280-1034

Counsel for Defendant Zackary Ellis Sanders

*****PUBLIC VERSION*****

TABLE OF CONTENTS

EXHIBITS INDEX

*****PUBLIC VERSION*****

Zackary Ellis Sanders, by and through undersigned counsel, and pursuant to Federal Rule of Criminal Procedure 41 and the Fourth Amendment, respectfully moves this Court to suppress all evidence and illegal fruits obtained pursuant to the invalid search warrant issued in this case. Mr. Sanders also respectfully moves for reconsideration of the Court's Order denying his Motion to Compel, which erroneously denied Mr. Sanders further evidence directly relevant to this Motion to Suppress.

INTRODUCTION

The Federal Bureau of Investigation ("FBI") was investigating a website called [redacted] Ex. 1 (Intel Log). [redacted]

[1] The FBI determined, through a [redacted] Mr. Sanders has requested [redacted] but the Government continues to withhold those documents.

[redacted], come anywhere close to establishing probable cause for a search warrant.

FBI Special Agent Christopher Ford ("the Special Agent") knew from [redacted] Agent [redacted]'s contemporaneous understanding of the limited nature of [redacted] The foregoing all make clear that the Court's finding in its August 21, 2020 Memorandum Opinion on Mr. Sanders's Motion to Compel [redacted] Memorandum Opinion (ECF No. 73) (emphasis added) at 10—was, respectfully, incorrect. [redacted]; it was not, however, an accurate statement of the Government's evidence, as the Special Agent well knew.

[2] The Affidavit refers to the [redacted] The Government has disclosed no communications from the FBI to the [redacted]—the documents that would most clearly convey the FBI's true understanding of the [redacted]'s tip and how that understanding conflicts with the Affidavit.

Once one understands the true limits of the Government's evidence at the [redacted] it is not hard to see how the FBI exploited [redacted],[3] misled the Magistrate about the state of the Government's evidence, and thereby obtained a warrant to search and seize every person, electronic device, room, garbage, treehouse, and vehicle on the family property [redacted] And in addition to capitalizing on the poor wording [redacted]

Additionally, the FBI included other misleading information [redacted] would draw the incorrect inferences necessary for finding probable cause. [redacted] In addition to [redacted]

[3] [redacted].

[redacted].

The FBI was also reckless as [redacted] While academics have discussed other methods that do not interfere with an Internet user's computer as being theoretically possible, [redacted] Ex. 11 (Third Declaration of Dr. Matthew Miller); Ex. 16 (Declaration of Dr. Richard Clayton). If the Special Agent was the expert he presented himself as, then he knew that to be the case. *See* Ex. 11 (Third Declaration of Dr. Matthew Miller) at 2; Ex. 16 (Declaration of Dr. Richard Clayton) at 8 [redacted], the Special Agent should have known [redacted]. *Id.* at 8-9. On the other hand, [redacted]

[redacted] The FBI cannot procure illegally obtained evidence [redacted] and then rely on it while misleading the Magistrate about how that evidence was obtained. Gov't Opp'n (ECF No. 41) at 16.

Based on the scant discovery the Government has provided to date, the Government's own statements, and the declarations submitted by four defense experts,[4] there is no question that Mr. Sanders has made "a substantial preliminary showing that a false statement knowingly and intentionally, or with reckless disregard for the truth, was included by the affiant in the warrant affidavit." *Franks v. Delaware,* 438 U.S. 154, 155–56 (1978). The Affidavit misled the Magistrate regarding the state of the Government's evidence [redacted] Particularly when the false statements are excised from the Affidavit and the material omissions are added, there was no basis for probable cause and no neutral Magistrate would have issued the warrant. As a result, Mr. Sanders requests, and is respectfully entitled to, a *Franks* hearing. *Id.* ("if the allegedly false statement is necessary to the finding of probable cause, the Fourth Amendment requires that a hearing be held at the defendant's request").

[4] The declarants are Dr. Matthew Miller, Associate Professor Computer Science and Information Technology at the University of Nebraska at Kearney; Matthew Ryder QC, U.K. barrister and part-time judge in higher criminal courts; Seth Schoen, computer technologist and privacy specialist who worked as a Senior Staff Technologist at the Electronic Frontier Foundation for the past 19 years; and Dr. Richard Clayton, Director of the Cambridge Cybercrime Centre at the University of Cambridge.

Because the warrant was based on materially false statements and omissions, and because *even without correcting the Affidavit* it was "so lacking in indicia of probable cause as to render official belief in its existence entirely unreasonable," *United States v. Leon*, 468 U.S. 897, 932 (1984), the *Leon* good faith exception does not apply. As a result, all evidence derived from the illegal search of the Sanders's family home, the interrogation of Mr. Sanders and his parents, and the forensic examinations of any tangible evidence should be suppressed as fruit of the poisonous tree.

PROCEDURAL HISTORY

A. The Search Warrant.

[redacted][5] That same day, the Magistrate issued a warrant for the FBI to search the Sanders's family home, [redacted]

On February 12, 2020, at 6:05 a.m., 26 law enforcement agents executed the invalid search warrant. The agents, with guns drawn, pulled Mr. Sanders's parents out of their home and forced Mr. Sanders at gunpoint into his mother's office. Ex. 8 [redacted] The FBI interrogated Mr. Sanders [redacted]

[5] [redacted]

[redacted]

B. Mr. Sanders's Initial Appearance, Detention Hearing, Indictment, and Arraignment.

On March 20, 2020, over five weeks later, Mr. Sanders was arrested and made his initial appearance.

On April 1, 2020, while litigating the issue of Mr. Sanders's detention, the Government represented that "[Mr. Sanders] came to the government's attention after an investigation conducted by the Federal Bureau of Investigation [] and other law enforcement entities revealed that an individual *accessed a website* that advertises child pornography[6] using an IP address associated with [Mr. Sanders's] residence in McLean, Virginia." Gov't Opp'n to Revocation of Detention Order (ECF No. 15) (emphasis added) at 2.

On June 24, 2020, based on the evidence derived from the illegal search of the Sanders's family home, Mr. Sanders was indicted on five counts of production of child pornography in violation of 18 U.S.C. § 225l (a) and § 2251(e), six counts of receipt of child pornography in violation of 18 U.S.C. § 2252(a)(2) and § 2252(b)(l), and one count of possession of child pornography in violation of 18 U.S.C. § 2252(a)(4)(B) and § 2252(b)(2). Mr. Sanders faces a mandatory minimum of fifteen years in prison for each count of production of child pornography.[7]

[6] [redacted]

[7] [redacted]

At arraignment on July 10, 2020, Mr. Sanders appeared before this Court and his counsel explained that he had a meritorious motion to suppress and for a *Franks* hearing, but that the Government was refusing to provide additional discovery in its possession, custody, or control relevant to that motion to suppress. The Court set a schedule for Mr. Sanders to submit a motion to compel and, once the Court had resolved that motion, a motion to suppress.[8]

C. Mr. Sanders's Motion to Compel Discovery.

On April 29, 2020, the Government, pursuant to its discovery obligations, produced the [redacted] On May 15, 2020, the Government produced the only other [redacted] On July 7, 2020, the Government produced two [redacted] Just several hours before filing its opposition to Mr. Sanders's Motion to Compel, the Government then produced a [redacted] Thus, with respect to the [redacted]

[8] On August 20, 2020, the Court extended the pretrial motions deadline to August 27, 2020.

[9] [redacted]

On July 13, 2020, and based on the Government's refusal to produce further discovery, Mr. Sanders moved to compel discrete categories of discovery. Mot. to Compel (ECF No. 37). The requested discovery would further establish that the Special Agent knew [redacted] *Id.* Mr. Sanders noted that he had submitted detailed discovery requests to the Government regarding the Government's contemporaneous understanding [redacted]. The Government, notwithstanding its obligations under Rule 16(a) and *Brady v. Maryland*, 373 U.S. 83 (1963), had refused to provide Mr. Sanders with meaningful discovery regarding the [redacted] This discovery was and is critical to Mr. Sanders's motion to suppress. *Id*. at 2.

On July 27, 2020, the Government filed an Opposition to Mr. Sanders's Motion to Compel Discovery. Gov't Opp'n (ECF. No. 41). Throughout the litigation of Mr. Sanders's motion, when [redacted] *See, e.g.,* Ex. 23 (July 31 Hearing Transcript) at 15, 20, 22, 24; Gov't Brief (ECF No. 53) at 1-3. The Government also repeatedly claimed [redacted] when there is no evidence that it did. None of the [redacted]

[redacted]

On August 10, 2020, Mr. Sanders and Government filed supplemental briefs. *See* Defense Brief (ECF No. 51); Gov't Brief (ECF No. 53). In its supplemental brief, the Government declined to explain to the Court [redacted] Again, although the Special Agent's contemporaneous understanding of the state of the Government's evidence [redacted] is the central issue underlying Mr. Sanders's Motion to Compel and this Motion, the Government did not have the Special Agent address that issue in his Declaration. *Id.*

On August 12, 2020, Mr. Sanders filed a response to the Government's Brief to make clear that [redacted] Mr. Sanders's response also noted that the "Government ha[d] presented an implausible, after-the-fact theory about how [redacted] Response to Gov't Brief (ECF No. 64).

D. The Court's Memorandum Opinion.

On August 21, 2020 the Court issued an Order (ECF No. 74) denying Mr. Sanders's Motion to Compel Discovery. In a Memorandum Opinion (ECF No. 73) accompanying the Court's Order, the Court rejected Mr. Sanders's central argument that the Government was in possession of further communications and documents relevant to Mr. Sanders's motion to suppress that it was refusing to produce. *Id.* at 9.

E. Mr. Sanders's Objections to the Court's Memorandum Opinion and Order.

On the issue of [redacted], the Court's Memorandum Opinion reflects a fundamental misunderstanding of Mr. Sanders's argument. The critical issue Mr. Sanders presented in his Motion to Compel (and also presents in this Motion) is not simply—as the Court characterized it—[redacted] *See* Memorandum Opinion (ECF No. 73) at 9 (finding that "Defendant's argument falters because defendant has not shown that any misrepresentation occurred here. [redacted]. While, as the Court later acknowledged in its Opinion, [redacted] was not—and is not—Mr. Sanders's central argument. Instead, Mr. Sanders's core argument is that, although the Special Agent [redacted] he knew that the imprecise language of the [redacted] was materially misleading, *as he knew that in repeating it, he conveyed to the Magistrate that* [redacted] The Special Agent's contemporaneous understanding is clear not just from the Special Agent's own [redacted], which characterizes the

extent of Mr. Sanders's activity as having [redacted] Tellingly, nowhere in any of the Government's previous filings did the Government ever represent that it believed then (or believes now) that it had actual evidence [redacted] That is the very reason why the Special Agent resorted to the [redacted] *Id.* (emphasis added). Accordingly, and respectfully, the Court's finding that "[redacted].[10] The Court's denial of Mr. Sanders's Motion to Compel

[10] [redacted]

accordingly violated his constitutional and statutory rights supporting further discovery on this issue and, if left to stand, will permit the Government to continue to conceal all further evidence of the Special Agent's culpable state of mind. That was not just incorrect legally but also fundamentally unfair to the defense so as to deny Mr. Sanders due process.[11]

[redacted]

[11] Respectfully, in addition to the Court's erroneous legal conclusion, the Court made a number of factual errors. [redacted]

Based on the Government's submissions when litigating Mr. Sanders's Motion to Compel, it is certain that the Government continues to withhold *Brady* and Rule 16 material that would further corroborate Mr. Sanders's position that the Special Agent knowingly and recklessly misled the Magistrate in multiple material respects. Indeed, despite having multiple opportunities to do so, including through a Declaration [redacted]. Instead, the Government has argued only that Mr. Sanders—a criminal defendant with no access to the Government's files—has not provided sufficient proof to "earn" discovery he has a right to in the first place. It is for these reasons that Mr. Sanders respectfully moves for reconsideration of the Court's ruling on his Motion to Compel, in the event the Court does not at this time grant his Motion to Suppress.

THE LAW OF *FRANKS v. DELAWARE*

In *Franks v. Delaware*, the Supreme Court set forth a two-step test for defendants to challenge the veracity of an affidavit in support of a search warrant. 438 U.S. 154, 155-56, 98 S. Ct. 2674 (1978); *accord United States v. Clenney*, 631 F.3d 658, 663 (4th Cir. 2011).

First, Mr. Sanders must "make[] a substantial preliminary showing that a false statement knowingly and intentionally, or with reckless disregard for the truth, was included by the affiant in the warrant affidavit, and if the allegedly false statement is necessary to the finding of probable cause, the Fourth Amendment requires that a hearing be held at the defendant's request." *Franks,* 438 U.S. at 155–56; *see also United States v. Leonard*, No. 17-cr-135, 2017 WL 4478330 at *5 (E.D. Va. October 6, 2017) (similar). "This showing must be more than conclusory and should include affidavits or other evidence to overcome the presumption of the warrant's validity." *Clenney*, 631 F.3d at 663 (quotation marks and internal punctuation omitted).

Second, at the *Franks* hearing, Mr. Sanders must establish "the allegation of perjury or reckless disregard . . . by a preponderance of the evidence." *Franks,* 438 U.S. at 156. Furthermore, "with the affidavit's false material set to one side, the affidavit's remaining content is insufficient to establish probable cause, the search warrant must be voided and the fruits of the search excluded to the same extent as if probable cause was lacking on the face of the affidavit." *Id.* at 156. "A warrant that violates *Franks* is not subject to the good-faith exception to the exclusionary rule." *Colkley*, 899 F.2d 297 at 300.

The Fourth Circuit has held that "[t]he *Franks* test also applies when affiants omit material facts "with the intent to make, or in reckless disregard of whether they thereby made, the affidavit misleading." *United States v. Colkley*, 899 F.2d 297, 300 (4th Cir. 1990); *see also Osborne v. Georgiades*, 697 F. App'x 234, 246 (4th Cir. 2017) ("To succeed on his claim, [the movant] must prove that [the affiant] deliberately or with a 'reckless disregard for the truth' made false statements of material fact in his affidavit, or omitted from that affidavit 'material facts with the intent to make, or in reckless disregard of whether they thereby made, the affidavit misleading'"). An omitted fact "is material if it is necessary to the neutral and disinterested magistrate's finding of probable cause;" in order words, if "its inclusion in the affidavit would defeat probable cause." *United States v. Wharton*, 840 F.3d 163, 168-169 (4th Cir. 2016) (quotation marks and punctuation omitted).

Mr. Sanders is entitled to a *Franks* hearing because this Motion makes the requisite substantial, non-conclusory, preliminary showing that the Special Agent misled the Magistrate with both deceptive statements and omissions on matters fundamental to probable cause. *Franks*, 438 U.S. at 171. The Fourth Circuit and District Courts therein have found *Franks* hearings warranted on far lesser showings. *See, e.g.*, *United States v. Tate*, 524 F.3d 449 (4th Cir. 2008)

(vacating the defendant's marijuana-related conviction and remanding for a *Franks* hearing when the defendant made a sufficient preliminary showing when the affiant officer omitted information about the location of the defendant's trash cans where the illegal marijuana was found); *United States v. Wharton*, No. ELH-13-0043, 2014 WL 3943358, at *1 (August 14, 2014), *aff'd United States v. Wharton*, 840 F.3d 163 (4th Cir. 2016) (granting a *Franks* hearing when an affiant officer executed a search warrant on the defendant's entire home but omitted information about the defendant occupying only a part of the home); *United States v. White*, No. 1:17-cr-94-1, 2017 WL 2633521, at *1 (M.D.N.C. June 19, 2017) (finding that the defendant made a preliminary showing that he was entitled to a *Franks* hearing based on a materially misleading statement in the affidavit, but a hearing was unnecessary because suppression was warranted on other grounds).

DISCUSSION

I. THE WARRANT WAS NOT SUPPORTED BY PROBABLE CAUSE.

A. BACKGROUND

The Special Agent's Affidavit contains one—and just one—allegation of criminal activity

[redacted]

Ex. 5 (Affidavit) at ¶ 23. While the Affidavit contains numerous other paragraphs documenting the Special Agent's background and experience, the Special Agent's [redacted]

[redacted]. *Id.* at ¶¶ 33-35. In stark contrast to cases where courts have upheld the Magistrate's probable cause determination, the Affidavit in this case did not describe specific content [redacted]

B. ARGUMENT

Assuming *arguendo* that the FBI did not knowingly or recklessly mislead the Magistrate or omit material facts from the Affidavit—which it did, *see infra*—the warrant issued in this case was invalid because it was not supported by probable cause to search the Sanders's family home or the electronic devices within it. Even without excising the false and misleading statements on which probable cause depended, and even when reviewing the Affidavit in the light most favorable to the Government, the facts the Special Agent presented in the Affidavit failed to provide "a fair probability that contraband or evidence of a crime w[ould] be found in a particular place." *Illinois v. Gates*, 462 U.S. 213, 238 (1983). The Affidavit contained "bare conclusions" that were insufficient to meet the probable cause standard. *Id.*at 239. As a result, the Magistrate did not have "a substantial basis for determining the existence of probable cause" that a search would uncover evidence of wrongdoing. *Id.* at 239.

A Magistrate is required to "make a practical, common-sense decision whether, given all the circumstances set forth in the affidavit before him, including the 'veracity' and 'basis of knowledge' of persons supplying hearsay information, there is a fair probability that contraband or evidence of a crime will be found in a particular place." *Gates*, 462 U.S. at 238. When a reviewing court examines the validity of a search warrant, such validity "must be assessed on the

basis of the information that the officers disclosed, or had a duty to discover and to disclose, to the issuing Magistrate," and not on what was uncovered afterwards during the execution of the warrant. *Maryland v. Garrison*, 480 U.S. 79, 85 (1987).

1. There was not probable cause to believe that the [redacted]

a. The Affidavit reflects no effort by law enforcement to corroborate the [redacted]

The Affidavit in this case rests *entirely* on [redacted]

The Special Agent's reiteration in [redacted] "mere affirmation of suspicion and belief without any statement of adequate supporting facts" that the Supreme Court has expressly rejected as providing an adequate basis for probable cause. *See Nathanson v. United States*, 290 U.S. 41, 46 (1933) (affiant's statement that he had "cause to suspect and does believe" that smuggled liquor was present in a private home was insufficient to provide probable cause). The Affidavit does not show [redacted]

[redacted]

The Affidavit does not contain sufficient facts to provide "a substantial basis for crediting the hearsay" [redacted], and that hearsay is not "reasonably corroborated by other matters" that were within the Special Agent's knowledge. *Jones v. United States*, 362 U.S. 257, 269 (1960), *overruled on other grounds by United States v. Salvucci*, 448 U.S. 83, 100 (1980).

There are no facts from which to determine how [redacted]

[redacted][12]

An informant's "veracity, reliability, and *basis of knowledge*" are "closely intertwined issues" to be considered as part of the totality of the circumstances when determining whether there is probable cause. *Gates*, 462 U.S. at 230 (emphasis added). In conducting such an analysis in *Illinois v. Gates*, the Supreme Court held that the corroboration of a tip "through other sources of information reduce[s] the chances of a reckless or prevaricating tale" and "thus provid[es] a substantial basis for crediting . . . hearsay." *Id.* at 244-245 (quoting *Jones v. United States,* 362 U.S. at 269, 271 (internal quotations omitted).

Here, however, [redacted] The Fourth Amendment dictates that "[s]ufficient information must be presented to the magistrate to allow that official to determine probable cause; his action cannot be a mere ratification of the bare conclusions of others." *Gates*, 462 U.S. at 239. [redacted]

[12] [redacted]

it is the type of bare-boned statement found in *Nathanson* and other similar cases to be insufficient for probable cause.

b. Without additional corroboration, [redacted].

The Affidavit is also notable for what it did not allege, but which would have been required for the Magistrate reasonably to infer [redacted]

There are at least five circumstances reflected in the Affidavit that made it unreasonable, [redacted]

[redacted][15]

c. There was not probable cause to believe [redacted]

Even assuming, *arguendo*, that there was probable cause to believe [redacted] *See, e.g.*, *United States v. Falso*, 544 F.3d 110, 120-21 (2d Cir. 2008) (finding no probable cause for possession of child pornography when it was alleged that defendant "appear[ed]" to have "gained access or attempted to gain access" to the cpfreedom.com website—which did not require registering an account or logging in—and that even if one inferred that the

[13] [redacted]

[14] [redacted]

[15] [redacted]

defendant had accessed cpfreedom.com, there was no specific allegation that the defendant "accessed, viewed or downloaded child pornography"); *see also, e.g. United States v. Doyle*, 650 F.3d 460, 472 (4th Cir. 2011) (finding no probable cause for possession of child pornography based on evidence of child molestation and claim from child victim that defendant showed the victim pictures of nude children).

Courts have required much more than the sparse facts contained in the Affidavit before finding probable cause. *See United States v. Bosyk*, 933 F.3d 319, 322 (4th Cir. 2019) (finding probable cause where FBI described message with hyperlink with numerous thumbnail images depicting man sexually molesting female toddler, which was unmistakably child pornography, and records subpoenaed from a file sharing site showed the defendant had viewed and clicked on that hyperlink to download child pornography), *cert. denied*, 140 S. Ct. 1124 (2020); *United States v. Richardson*, 607 F.3d 357 (4th Cir. 2010) (finding probable cause where investigation linked defendant's email accounts, which he used to distribute child pornography, to the address where the warrant was executed); *United States v. Bynum*, 604 F.3d 161 (4th Cir. 2010) (finding probable cause where someone with a particular screen name at address where warrant was executed had uploaded suspected child pornography to the Internet); *United States v. Goodwin*, 854 F.2d 33 (4th Cir. 1988) (finding probable cause for anticipatory search warrant when defendant ordered child pornography and investigation verified that materials would be delivered to address where warrant was executed); *United States v. Bailey*, 272 F. Supp. 2d 822, 824 (D. Neb. 2003) (finding probable cause where someone using a particular e-mail address knowingly subscribed to a specialized Internet site that distributed child pornography); *United States v. Shields*, No. 4:CR-01-0384, 2004 WL 832937, at *7 (M.D. Pa. Apr. 14, 2004), *aff'd*, 458 F.3d 269 (3d Cir. 2006) (finding probable cause where it was clear that the defendant voluntarily subscribed to and joined two websites

whose purpose was to share child pornography); *United States v. Froman*, 355 F.3d 882, 890–91 (5th Cir. 2004) (finding probable cause where the defendant paid to join a group called Candyman where the sole purpose was to receive and distribute child pornography, the defendant registered screennames that reflected an interest in child pornography, and the defendant did not cancel his paid subscription to the group); *United States v. Hutto*, 84 F. App'x 6, 8 (10th Cir. 2003) (finding probable cause where the defendant paid to join a group where images of child pornography were available to all members).

[redacted]

Cf. United States v. Bosyk, 933 F.3d 319, 322 (4th Cir. 2019) (in affidavit, FBI alleged defendant clicked on with numerous thumbnail images depicting man sexually molesting female toddler), *cert. denied*, 140 S. Ct. 1124 (2020). [redacted]

[redacted]

Generalized statements [redacted] are not probative of the required intent. Thus, [redacted]

[redacted]

d. The warrant was stale.

The FBI did not have probable cause to search the Sanders's family home in February 2020, [redacted]

C. THE GOOD FAITH EXCEPTION DOES NOT APPLY.

The good faith exception to the exclusionary rule does not apply here. *See United States v. Leon*, 468 U.S. 897 (1984). The Fourth Circuit has held:

> The *Leon* good-faith exception is not available where (1) probable cause is based on statements in an affidavit that are knowingly or recklessly false; (2) the magistrate fails to perform a "neutral and detached" function and instead merely rubber stamps the warrant; [or] (3) the affidavit does not provide the magistrate with a substantial basis for determining the existence of probable cause.

United States v. Gary, 528 F.3d 324, 329 (4th Cir. 2008).

Even assuming *arguendo* that the Special Agent did not knowingly or recklessly mislead the Magistrate, *the Magistrate failed to perform its neutral and detached function* because the Magistrate merely rubber-stamped the bare conclusions o[redacted] Finally, even without the excised false statements and with the material information that the Special Agent omitted, the *Affidavit did not provide a substantial basis for probable cause***.** This Court has held that "a magistrate may rely on law enforcement officers, who may draw on their own experience and specialized training to make inferences from

and deductions about the cumulative information available to them that might well elude an untrained person, *as long as the affidavit contains facts to support the law enforcement officer's conclusions*." *United States v. Matish*, 193 F. Supp. 3d 585, 602 (E.D. Va. 2016) (citing *United States v. Johnson*, 599 F.3d 339, 343 (4th Cir.2010)) (internal citations and quotations omitted) (emphasis added). In this case, for the reasons previously discussed, *see supra*, there were insufficient facts to support the [redacted]

II. THE SPECIAL AGENT KNOWINGLY MISLED THE MAGISTRATE IN [redacted]

The Affidavit contains just one allegation of criminal activity [redacted]

A. BACKGROUND

[redacted]

[redacted]

[16] [redacted]

[redacted]

[redacted]

[redacted]

18 [redacted]

[redacted]

[19] [redacted]

[redacted]

[redacted]

[redacted]

[redacted]

---

[20] [redacted]

[21] [redacted]

[redacted]

3. How the Special Agent Described [redacted]

[redacted]

b. The Affidavit (Paragraphs [redacted]

[redacted]

Ex. 5 (Affidavit) [redacted]

[22] [redacted]

[redacted]

Ex. 5 (Affidavit) at [redacted]

[redacted]

[redacted]

B. ARGUMENT

"[W]hen the Fourth Amendment demands a factual showing sufficient to comprise probable cause, the obvious assumption is that there will be a truthful showing." *Franks v. Delaware*, 438 U.S. 154, 164–65 (1978) (quotation marks and citations omitted). This showing must be "truthful . . . in the sense that the information put forth is believed or appropriately accepted by the affiant as true." *Id.* at 164-165. Furthermore, "[b]ecause it is the magistrate who must determine independently whether there is probable cause, . . . it would be an unthinkable imposition upon his authority if a warrant affidavit, revealed after the fact to contain a deliberately or reckless false statement, were to stand beyond impeachment." *Id.* at 165.

Under no interpretation of the *Franks* caselaw may an affiant include a tip—whether from a confidential informant or another law enforcement agency or from any other source—he knows is misleading on its face and then "omit" information in the affiant's possession regarding why that tip inaccurately describes the evidence. *Id*. at 156 (finding an omission material if it is "necessary to the [neutral and disinterested magistrate's] finding of probable cause"); *Colkley*, 899 F.2d 297 at 300 ("*Franks* protects against omissions that are designed to mislead, or that are made in reckless disregard of whether they would mislead, the magistrate"); *United States v. Wharton*, 840 F.3d 163, 168–69 (4th Cir. 2016) (finding "a law enforcement officer's reckless omission of facts from his affidavit, which undermined the reliability of a confidential informant, were material"); *Miller v. Prince George's Cty., MD*, 475 F.3d 621, 629 (4th Cir. 2007) ("selectively includ[ing] information bolstering probable cause, while omitting information that did not . . . can mislead a magistrate by reporting less than the total story, thereby manipulating the inferences a magistrate will draw"); *United States v. Taylor*, 935 F.3d 1279, 1302-03 (11th Cir. 2019) ("If the officials who sought the warrant are culpable for misleading the magistrate, the fault lies with them. And the object of suppression would be to deter law enforcement from misleading magistrates in the future, not to prevent warrants like this one from issuing"); *United States v. McLamb*, 880 F.3d 685, 690 (4th Cir. 2018) ("In *Leon*, the Supreme Court explained the limits of the good faith exception: 'Suppression . . . remains an appropriate remedy if the magistrate or judge in issuing a warrant was misled by information in an affidavit that the affiant knew was false or would have known was false except for his reckless disregard of the truth.'").

[redacted]

[redacted]

[23] [redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted] These omissions if "included would defeat a probable cause showing" and "w[ere] designed to mislead or w[ere] made with reckless disregard of whether [such omissions] would mislead." *United States v. Tate*, 524 F.3d 449, 455 (4th Cir. 2008).

[redacted]

[redacted]

This was obvious for at least five reasons. [redacted]

[redacted]

III. THE SPECIAL AGENT KNOWINGLY MISLED THE MAGISTRATE ABOUT TOR AND OTHER ISSUES MATERIAL TO PROBABLE CAUSE.

In addition to [redacted] the Affidavit included other deliberately misleading or irrelevant information, and omitted material facts, in order to further ensure that the Magistrate drew the incorrect inferences necessary for finding probable cause. The Affidavit misled the Magistrate about [redacted]

A. BACKGROUND

1. The Tor Network

"Tor" originally stood for "The Onion Routing,"[24] because the network provides security by encasing data that travels through the network in different layers of encryption, like an onion: these layers of encryption are gradually unpeeled at different points in the random circuit of at least three of the thousands of volunteer-run nodes around the world that comprise the Tor network. *See* Ex. 16 (Declaration of Dr. Richard Clayton) at 3-4 (explaining how data that travels on the Tor network is encrypted in what is best analogized as a "three-layer 'onion'"). As this Court has previously acknowledged, "[t]he U.S. Naval Research Laboratory created the Tor network in an attempt to protect government communications. The public now can access the Tor network.

[24] *History*, the Tor Project, https://www.torproject.org/about/history/ (last accessed Aug. 18, 2020).

Many people and organizations use the Tor network for legal and legitimate purposes." *United States v. Matish*, 193 F. Supp. 3d 585, 593 (E.D. Va. 2016).

The Tor network "provides anonymity to users of the network" through at least three random nodes that comprise what is called a Tor circuit. Ex. 12 (Fourth Declaration of Dr. Matthew Miller) at 2-3. Thus, "[w]hen someone visits a web site using the Tor Browser, all the communications with the web site are sent through . . . three or more randomly chosen Tor nodes, out of the thousands that make up the Tor network, passing through them before arriving at their destination." Ex. 15 (Declaration of Seth Schoen) at 1-2.

The way the Tor network works when an Internet user browses the Internet on the Tor network is best explained by an analogy to mail: "[t]he routing of the packets [of data] from the Internet user, through the Tor circuit, to a website is like opening an envelope, which contains 2 other progressively smaller envelopes, the last of which contains the request to be sent to the website." Ex. 12 (Fourth Declaration of Dr. Matthew Miller) at 2. However, in this analogy, "[e]ach envelope does not reveal the recipient or the contents of the next smaller envelope." *Id.* at 2. Thus, as Dr. Miller explains in further detail:

> When an Internet user visits a website through the Tor Network, the Internet user's request is sent to that website by traveling from the Internet user to node 1, from node 1 to node 2, from node 2 to node 3, and then from node 3 to the website. When the Tor Browser sends packets of data through the Tor Network, it has to encrypt the packets of data in the reverse order they travel in. The Internet user's request (packets of data) to the website is placed on an un-encrypted postcard (Postcard #1), where the return address is node 3 and the recipient address is to the website. Postcard #1 is encased in an encrypted envelope (Envelope #3), where the return address is node 2 and the recipient address is node 3. Envelope #3 is encased in an encrypted Envelope #2, where the return address is node 1 and the recipient address is node 2. Envelope #2 is encased in an encrypted Envelope #1, where the return address is the Internet user and the recipient address is node 1.

Id. at 2.

Dr. Richard Clayton provides "a real-world example of what one node within a TOR network does" to further illustrate this process:

> an anonymous Valentine can be sent by putting the card into an envelope and addressing it to its destination. This can then be put into another envelope and sent to a small town in Texas. The outer envelope will be opened and the post office will frank the inner envelope "Valentine, TX" and the card will then be delivered by the Post Office to its destination. Inspecting the outer envelope does not reveal the inner envelope's destination – and the card's recipient does not know in which town the sender resides. Further, since envelopes come in a small range of standard sizes, someone watching all the mail would not be able to track any particular envelope merely by measuring it.

Ex. 16 (Declaration of Dr. Richard Clayton) at 4.

While "the Tor network's privacy features make it more difficult to count its users compared to other software and services, available statistics suggest that the Tor network is currently used by about 2.5 million people each day." Ex. 15 (Declaration of Seth Schoen) at 2; *see also* Ex. 16 (Declaration of Dr. Richard Clayton) at 7 (similar).

2. The Tor Project

The Tor Project is a 501(c)(3) non-profit organization that supports the Tor network and the Tor Browser to protect freedom online. The Tor Project's mission is "[t]o advance human rights and freedoms by creating and deploying free and open source anonymity and privacy technologies, supporting their unrestricted availability and use, and furthering their scientific and popular understanding."[25] As part of the mission, the Tor Project was "the main developer of the Tor Browser and the software behind the Tor Network." Ex. 15 (Declaration of Seth Schoen) at 1. The Tor Project developed the Tor Browser to provide the public with easy access to the Tor

[25] *Browse Privately. Explore Freely*, The Tor Project, https://www.torproject.org/ (last accessed Aug. 13, 2020); Ex. 15 (Declaration of Seth Schoen) at 2; Ex. 12 (Fourth Declaration of Dr. Matthew Miller) at 3.

Network and heightened anonymity protections when browsing online. *Id.* Today, the Tor Project promotes, supports and provides downloads for the Tor Browser. *Id.*

a. The U.S. Government is and has been one of the main sponsors of the Tor Project.

The U.S. government has been one of the main proponents and supporters of Tor. The first onion routing network design and prototype was created by the U.S. Naval Research Laboratory in the mid-1990s.[26] It was designed to provide Internet users with maximum privacy by routing Internet traffic through multiple servers. Since then, other researchers, developers, and organizations have sought to build on that work, most notably the Tor Project. In 2006, the Tor Project obtained its 501(c)(3) status and The Tor Project was established as a non-profit to support the development of the Tor network and the Tor Browser. The Tor Project has been heavily funded by the U.S. government "to promote Internet freedom." Ex. 15 (Declaration of Seth Schoen) at 2.

Some of the active sponsors who fund The Tor Project's work today include the U.S. government, educational institutions, philanthropies, and well-known publicly traded companies. For example, current active sponsors include the U.S. Department of State Bureau of Democracy, Human Rights, and Labor; the Media Democracy Fund; the Defense Advanced Research Projects Agency via Georgetown University; the National Science Foundation via Georgetown University; the Institute of Museum and Library Services via New York University; Craig Newmark Philanthropies; and the Google Summer of Code program.[27]

b. Neither the Tor Network nor the Tor Browser are designed or primarily used for illegal purposes.

---

[26] *History*, the Tor Project, https://www.torproject.org/about/history/ (last accessed Aug. 18, 2020).

[27] *Sponsors*, The Tor Project, https://www.torproject.org/about/sponsors/ (last accessed Aug. 13, 2020); *see also* Ex. 15 (Declaration of Seth Schoen) at 2 (similar).

Neither the Tor network nor the Tor Browser are designed or primarily used for illegal activities. Rather, "Tor has been developed to be a tool for free expression, privacy, and human rights. It is not a tool designed or intended to be used to break the law, either by Tor users or Tor relay operators."[28] Indeed, the vast majority of people (over 96%) who use the Tor network and Tor Browser do so to visit websites on the open Internet with the heightened anonymity protections that Tor provides. "[H]idden service traffic is about 3.4 percent of total Tor traffic, which means that, at least according to our early calculations, 96.6 percent of Tor traffic is []not[] hidden services . . . In other words, the majority of Tor traffic comes from users that are using the network to browse the public-facing web anonymously, and not by those accessing hidden sites").[29] Of the less than four percent of Tor Onion Service websites that make up traffic on the Tor network, the majority of such websites (52%) are legal under both U.S. and U.K. law.[30]

3. The Tor Browser

The Tor Browser is a software application that people use to access the Tor network and thereby browse websites on both the open Internet (what people usually think of when they think of the Internet) and Tor Onion service websites. *See, e.g.*, Ex. 9 (Declaration of Dr. Matthew Miller) at 2 ("The Tor Browser is a browser that uses the Tor Network to connect to the Internet. It has the ability to browse 'open' Internet websites as well as Tor Onion Service websites"). When [redacted] Internet users could

[28] *The Legal FAQ for Tor Relay Operators*, the Tor Project, https://community.torproject.org/relay/community-resources/eff-tor-legal-faq/

[29] Matthew Braga, *Most Tor Traffic isn't going to the Dark Web, Data Suggests*, Vice (Feb. 27, 2015), https://www.vice.com/en_us/article/9ak8av/most-tor-traffic-isnt-going-to-the-dark-web-data-suggests (quotation marks omitted).

[30] Larry Loeb, *Study Shows Dark Web Isn't as Large or Illegal as Previously Thought*, Security Intelligence (Apr. 12, 2016), https://securityintelligence.com/news/study-shows-dark-web-isnt-as-large-or-illegal-as-previously-thought/.

visit it, other Tor Onion Service websites, or open Internet websites by connecting to the Tor network through the Tor Browser.

a. There are many legitimate reasons for people to use the Tor Browser to connect to the Tor network.

Protecting the anonymity of a user's IP address is a design feature of both the Tor network and the Tor Browser, and it is what provides people with many legitimate reasons for downloading and using the Tor Browser to access the Tor network. Ex. 15 (Declaration of Seth Schoen) at 4. Because people's activities online can otherwise be tracked, people who want to control what information they share about themselves can use the Tor Browser to make sure their information isn't exposed or tracked in ways they don't want." *Id.* at 2. For example, people may use Tor to protect their anonymity because:

> Many people don't want the things they say online to be connected with their offline identities. They may be concerned about political or economic retribution, harassment, or even threats to their lives. Whistleblowers report news that companies and governments would prefer to suppress; human rights workers struggle against repressive governments; parents try to create a safe way for children to explore; victims of domestic violence attempt to rebuild their lives where abusers cannot follow.[31]

Anonymizing online activities can enable people to more freely communicate, organize, and associate with others. Using a Tor browser can create space for people to develop and share ideas. In particular, people who are members of minority groups who may fear discrimination or harassment on the basis of their sexual orientation, ethnicity, race, religion, or gender identity can feel more empowered to exercise their First Amendment rights in such spaces. *See, e.g.*, *McIntyre v. Ohio Elections Comm'n*, 514 U.S. 334, 357 (1995) (explaining, in a different context, how "[a]nonymity is a shield from the tyranny of the majority. . . . It thus exemplifies the purpose

[31] *Anonymity,* Electronic Frontier Foundation, https://www.eff.org/issues/anonymity (last accessed Aug. 19, 2020).

behind the Bill of Rights, and of the First Amendment in particular: to protect unpopular individuals from retaliation—and their ideas from suppression—at the hand of an intolerant society").

As another example of why people would legitimately use the Tor Browser, it helps people keep private information that companies would otherwise seek to collect to profile people and target advertisements towards them. If people want to search for sensitive information, such as information about "erectile dysfunction, herpes, adult incontinence, bankruptcy, gay bars, BDSM, fertility issues, pregnancy, or abortion," if they use the Tor Browser to search for such information it will help "break the connection between the sensitive topic and the identity of the person doing the search" and thereby avoid "repeatedly being shown uncomfortably revealing ads on the topic in the future." Ex. 15 (Declaration of Seth Schoen). at 2. In addition to using the Tor Browser to keep private personal information and avoid targeted ads, people also use it to keep their location private, see what websites look like from elsewhere in the world, avoid Internet censorship, do research without revealing where they work, and provide anonymous tips to media or law enforcement. *Id.* at 3-4. People use Tor for these reasons precisely because Tor allows people to keep their identity and activities private by protecting the anonymity of the IP addresses of the devices they use. *Id.* at 4.

b. The Tor Browser is a non-default browser (like Google Chrome or Mozilla Firefox) but, compared to other browsers, it has heightened privacy and security protections.

The Tor Browser is a non-default browser that allows people to easily access the Internet and make choices about what they reveal about themselves—and what they do not—to advertisers, private corporations, data brokers, websites, and anyone else who is otherwise monitoring, drawing inferences from, and even profiting off of people's activities online. *Id.* at 2-4; *see also*

Ex. 12 (Fourth Declaration of Dr. Matthew Miller) at 3. It is similar in some ways to other web browsers, like Internet Explorer, Apple Safari, Mozilla Firefox, Google Chrome, and Microsoft Edge, in that it allows Internet users to access the Internet. Indeed, the Tor Browser is actually an enhanced version of Mozilla Firefox. Ex. 15 (Declaration of Seth Schoen) at 4; Ex. 16 (Declaration of Dr. Richard Clayton) at 5. Non-Tor browsers, such as the ones previously described, lack the heightened privacy and security settings of the Tor Browser. The Tor Browser allows Internet users to access (via the Tor network) both open Internet websites and Tor Onion Service websites.

Like Mozilla Firefox and Google Chrome (but unlike Internet Explorer, Apple Safari, or Microsoft Edge), the Tor Browser is a non-default web browser, which means that it does not automatically come installed on a device when someone purchases it. People who want to use a non-default browser need to take affirmative steps to download one.

The Tor Browser is considered a better browser than the default browsers that automatically come with devices (such as Internet Explorer, Apple Safari, or Microsoft Edge) and better than other non-default browsers (such as Mozilla Firefox and Google Chrome). For example, Fox News compared which was the best of different web browsers and gave the Tor browser an honorable mention: Fox News reported that the "Tor Browser is one of the best anonymous web browsers out there. It's so reliable, in fact, that people living under repressive governments have used it to break through censorship. . . if you're looking for the safest, most private way to browse the net, Tor might be your go-to."[32] Furthermore, Fox News noted that while Apple Safari and Microsoft Edge are the "default" browsers that usually "come bundled with new computers, . . . they tend to lack some of the security features and extensions" found in other

[32] *Which browser is best? Comparing Chrome, Safari, Firefox, Edge, and Tor*, Fox News, https://www.foxnews.com/tech/which-browser-is-best-comparing-chrome-safari-firefox-edge-and-tor (last accessed Aug. 13, 2020).

browsers one can download.[33] Fox News further counselled against using a default browser such as Internet Explorer, giving it a dishonorable mention, in part because it is "an absolute minefield for malware."[34]

The Tor Browser has heightened privacy and security for a number of reasons. It allows an Internet user to browse the Internet via the Tor network. It "does not (1) save an Internet user's search history in the browser itself as the Internet user is browsing or (2) save search history or cache images to the hard disk of the Internet user's computer," in order to ensure "that an Internet user does not reveal their search history or what they have done on the Internet" and thereby "protect [an] Internet user's anonymity." Ex. 12 (Fourth Declaration of Dr. Matthew Miller) at 3. It also "severely restrict[s]" the functionality of "code (especially JavaScript code) embedded into websites" in order to protect the anonymity of an Internet user's IP address. Ex. 16 (Declaration of Dr. Richard Clayton) at 5.

c. The Tor Browser is easy to download.

It is simple for anyone to download the Tor Browser—even if they are not technically sophisticated—on their computer, mobile phone, or other web-accessible device. Ex. 15 (Declaration of Seth Schoen) at 4. For example, a person can go to the Tor Project website, at https://www.torproject.org/download/, and with one or two clicks[35] download the Tor Browser for free. Downloading the Tor Browser from the Tor Project website takes no more than a few minutes.

---

[33] *Id.*

[34] *Id.*

[35] Some browsers (and depending on how people have configured their browsers) will ask a person to confirm that they want to download a file, while others will immediately start downloading after a person click the download button.

Ex. 15 (Declaration of Seth Schoen) at 5-6 (describing the steps required to download the Tor Browser and providing screenshots to provide a visual explanation).

d. The steps required to download the Tor Browser are the same steps required to download any other non-default browser.

Downloading a web browser is the same process whether someone is downloading the Tor Browser or another non-default browser like Mozilla Firefox or Google Chrome. *Id.* at 4 ("The steps to download and use the Tor Browser are the same as those to download and use any other Browser"); *see also id.* at 5-6 (depicting and explaining the steps required to download the Tor Browser).[36]

e. The Tor Browser is easy to use.

The Tor Browser was specifically designed to be as easy to use as any other non-default browser, so that the public could have free, easy-to-access, heightened security protections while browsing online. *Id.* at 4; *see also* Ex. 16 (Declaration of Dr. Richard Clayton) ("Using TOR is extremely easy – one downloads the 'TOR bundle for Windows, Mac or for one's phone or tablet. One then installs it and launches it and it can immediately be used. On a fast connection this takes less than a minute"). Once a person has downloaded the Tor Browser, to browse the Internet they simply need to open the program by clicking on its icon—just like they would for any other web browser. Ex. 15 (Declaration of Seth Schoen). at 7. "The Tor Project has continued to improve

[36] If someone wanted to download Google Chrome or Mozilla Firefox, someone would simply need to search for "Google Chrome" or "Mozilla Firefox" in a search engine and then follow the same steps as described in Ex. 15 (Declaration of Seth Schoen), *i.e.* they would simply visit the relevant download page and download the software.

the ease of use and security of the Tor Browser since 2008. These enhancements to the Tor Browser are one of the Tor Project's core activities." *Id.* at 4.

One a person has opened the Tor Browser, it is similar to any other web browser. *See Id.* at 7 (providing a screenshot of the Tor Browser). There is a web address bar where a person can enter the address of the website they want to visit. *Id.* There is also a default search engine bar where a person can enter search terms. *Id.* For example, if a person used the default search engine bar, they could search for, for example, "eastern district of virginia u.s. district court" and the search engine would display the results. *See Id.* at 8 (providing a screenshot of search results on the Tor Browser). A person could then use the Tor Browser to visit this Court's website. *See Id.* at 9 (providing screenshot of the "Court's website as visited with the current version of Tor Browser" and noting "[t]he process of navigating to it, and the site's appearance, were much the same as in any other web browser"). There is also a search engine for Tor Onion Service websites, called Torch, which Internet users can find simply by searching "Tor search engine." A person could search for, for example, "department of justice" results on Tor Onion Service websites. *See Id.* at 12 (providing a screenshot of search results on the Tor Browser).

4. How People Browse the Internet.

When people "browse" the Internet, they do not always know what they are looking for: in fact, the very phrase "browsing the Internet" can "imply a sense of aimlessness, with the user just wasting time on the Internet."[37] Thus, "[b]ecause of how Internet users browse the Internet there are two main ways that they usually come across a website: 1) by using a search engine or 2) by clicking on a hyper-link (aka a link)." Ex. 12 (Fourth Declaration of Dr. Matthew Miller) at 6. People can and do click on links or even register for accounts without knowing where it will

[37] *Browsing*, Technopedia, https://techopedia.com/definition/797/browsing (last accessed Jul. 29, 2020).

lead them. Ex. 10 (Second Declaration of Dr. Matthew Miller) at 2; *see also* Ex. 15 (Declaration of Seth Schoen) ("Internet users can easily visit web sites without knowing their contents, whether by clicking on search engine results or following a link that they found or received in some other way"). "Within Tor Browser, links to onion sites can be used and visited just like other web sites. For example, a Tor Browser user can navigate to one simply by clicking on a search engine result or other link." *Id.* at 11.

a. Search engines.

People can use search engines to browse the open Internet and Tor Onion Service websites. *See, e.g.*, Ex. 15 (Declaration of Seth Schoen) at 11-12. Indeed, "there are search engines that do 'index' the contents of the Tor Network, including Tor Onion Services. Search engines create indexes which are like the yellow pages of the Internet. These indexes provide a brief description of the webpages, but search engines usually do not have access to password protected pages on a website. Thus, they usually cannot view or describe the content that is password protected." Ex. 12 (Fourth Declaration of Dr. Matthew Miller) at 6-7.

When people use a search engine, such as Google, DuckDuckGo, or Torch, it is "not unusual for Internet users to receive search results that are different from what they expected, or to be confused about the nature of a particular search result, or to click on a search result that's not what they intended." Ex. 15 (Declaration of Seth Schoen) at 10. This is because "[m]any words and terms have multiple possible meanings, and these ambiguities create challenges for search engines and Internet users." *Id*. at 10. "For example, an Internet user might search for 'cardinals' or 'pictures of cardinals'. They might find or click on web sites dedicated to various kinds of cardinals: a common bird in North America, the St. Louis Cardinals baseball team, or the members of the College of Cardinals in the Roman Catholic Church." *Id.* at 10. Furthermore, search engine

results for websites that require a login may not be accurate or make clear what the website will contain: "content that requires special access such as a login account is almost always invisible to web crawlers, and so not indexed by search engines and invisible to Internet users. For example, a search engine couldn't see the content of a private discussion forum that required a login." *Id.* at 10. (However, while the search engine's description of a website that requires a login to view will not be accurate because the password-protected content is invisible to the search engine, and therefore Internet users looking at search results, the website itself would still be indexed by the search engine).

b. Links.

"Users can, not uncommonly, get a [URL] link from a search engine or from another source and click on it without knowing any or all of the content that they'll find on that particular page." Ex. 15 (Declaration of Seth Schoen) at 11. People may not know where a URL link will lead because links are often "opaque," meaning "there's no way to tell what they lead to just by looking at them." *Id.* at 11. A couple of examples help illustrate this point:

- "[B]oth of the video links https://www.youtube.com/watch?v=0Ak_7tTxZrk and https://www.youtube.com/watch?v=2mBF2gSEEHQ have a very similar appearance, with a meaningless data element at the end ("0Ak_7tTxZrk" and "2mBF2gSEEHQ"). One of these videos is a performance of a Beethoven piano sonata, while the other is footage of the August 2020 explosion in the port of Beirut." *Id.* at 10-11.
- "[O]ne of https://bit.ly/2XRd3IU and https://bit.ly/3izBkv8 will send Internet users to this Court's web site, while the other points them to a Rick Astley music video." *Id.* at 11.
- [redacted]

that website. *See Id.* at 13; *see also* Ex. 17-18 [redacted] Indeed, even the [redacted] Ex. 15 (Declaration of Seth Schoen) at 10; *see also supra* at n.18.

In addition to URL addresses being ambiguous, hyperlinks can also be ambiguous. Hyperlinks "provide[] only a short description of where the user will go, but there could be different content hosted at the website. A common example would be the use of headlines in a newspaper article, where the headline would grab the reader's attention, but only when they read the article, will they know the true story. A [hyper]link (like a headline) is a word or short phrase that cannot fully represent the content the user will view after clicking on the link." Ex. 12 (Fourth Declaration of Dr. Matthew Miller) at 6. Thus, "[f]or example, a pornography website could be [hyper-]linked (described) as a BDSM website and just based on the text displayed to the Internet user, they would not know exactly what content they would find if they clicked on the [hyper-]link to that website." *Id.* at 6.

c. A One-Time Visit to a Website.

"Someone who visits a web site only once is more likely to have found the content of that site was either not what they expected or not what they were looking for, compared to someone who visits a web site repeatedly." Ex. 15 (Declaration of Seth Schoen) at 10.

B. ARGUMENT

1. The Affidavit misled the Magistrate about Tor.

The Affidavit misled the Magistrate about Tor in paragraphs [redacted]

[redacted]

[redacted] downloading and installing the Tor Browser requires the same steps (and is just as easy) as downloading and installing a non-default browser. Additionally, the steps required "to download the Tor Browser and access the Tor network are the same steps that a user would take in order to make use of Tor for any of the legitimate reasons" previously described. Ex. 15 (Declaration of Seth Schoen) at 5. [redacted] of the origins of Tor, the mission and purpose of the Tor Project, the U.S. government's connection to the Tor network and Tor Project as a key sponsor and supporter, the many legitimate reasons that people download and use Tor, and the benefits that Tor provides in terms of anonymization that are not primarily intended to shield illegal activity.

The Affidavit's misleading statements and omissions [redacted] are material because the Affidavit was incorrectly asking the Magistrate to read suspicion into legitimate conduct that many people engage in every day. Had the Affidavit provided a more accurate and complete characterization of Tor, the Magistrate would have had a more complete understanding of why and how people use Tor and would have ultimately understood that [redacted]

[redacted]

[redacted] The Affidavit misled the Magistrate about [redacted].

[redacted]

[redacted]. *See, supra* at 27-29. [redacted]

3. The Affidavit misled the Magistrate about [redacted]

The Affidavit misled the Magistrate [redacted]

[redacted]

[redacted]

4. The Affidavit misled the Magistrate about evidence [redacted]

[redacted]

[redacted]

5. The Affidavit misled the Magistrate [redacted]

The Affidavit misled the Magistrate [redacted]

[redacted]

6. The Affidavit misled the Magistrate by omitting information [redacted]

The Affidavit misled the Magistrate by failing to disclose [redacted]

[redacted]

7. The Affidavit misled the Magistrate through omissions that, taken together, were essential for the Magistrate to find probable cause.

As discussed elsewhere in this Motion, the Affidavit did not disclose to the Magistrate about information that, individually and especially when taken together, would have prevented the Magistrate from finding probable cause. For example, the Special Agent did not tell the Magistrate that: [redacted]

IV. THE SPECIAL AGENT RECKLESSLY MISLED THE MAGISTRATE IN [redacted]

The FBI, based on the information that it received [redacted]

[redacted]

A. BACKGROUND

[redacted]

[redacted]

[redacted]

In the Eastern District of Virginia, FBI Special Agent Douglas Macfarlane swore two Affidavits for search warrants to deploy an NIT on a target website to seize the true IP addresses of people who logged into the website by entering a username and password. He stated:

> Due to the unique nature of the Tor network and the method by which the network protects that anonymity of its users by routing communications through multiple other computers or 'nodes,' . . . *other investigative procedures that are usually employed in criminal investigations of this type have been tried and failed or reasonably appear to be unlikely to succeed if they are tried*. . . . Under the NIT authorized by this warrant, the TARGET WEBSITE . . . would augment that content [that websites send to visitors in the normal course of operation] with additional computer instructions . . . designed to cause the user's 'activating' computer to transmit certain information to a computer controlled by or known to the government. . . . *to the extent that use of the NIT can be characterized as a seizure* of an electronic communication or electronic information, . . . such a seizure is reasonably necessary, because *without this seizure, there would be no other way, to my knowledge, to view the information and to use it to further the investigation*.

United States v. Matish, 193 F. Supp. 3d 585 (E.D. Va. 2016) (ECF No. 18-2 at 24-25, 29) (emphasis added);[39] *see also United States v. Darby*, 190 F. Supp. 3d 520 (E.D. Va. 2016) (ECF No. 23-2 at 27-28, 32) (exact same) (emphasis added).

FBI agents have testified to the same in court. As FBI Special Agent Steven Smith previously testified:

> In the case of a Tor hidden service, once we seize that website, we don't know the true IP address of the users, so we're not able to trace back who those users are. We only would be able to see, at most, the last node in the connection. That would be the IP address available to us. And we would not be able to trace back to the originating IP address. . . . *We have to have a method in which we can proactively, once we seize the website, attempt to ascertain the user's true IP address* and *we typically do this through network investigative technique . . . to cause the user's computer to communicate with an FBI-controlled computer outside the Tor network*.

[39] Special Agent Douglas McFarlane's affidavit in *U.S. v. Matish* contains a significant amount of language that is extremely similar and in some cases identical [redacted]. *Compare* Ex. 121(*Matish* Affidavit) *with* Ex. 5 (Affidavit); *see also* Ex. 22 [redacted]

United States v. Cottom, No. 8:13CR108, 2013 WL 6567553 (D. Neb. Dec. 12, 2013) (ECF No. 257 at 21) (emphasis added).

FBI Special Agent Daniel Alfin, who was the case agent for the national Playpen investigation in multiple jurisdictions, previously testified that it was "correct" that when Internet users "access[ed] the site using the Tor Browser . . . *you're required to send some kind of additional exploit to get code to execute on their computer . . . because of a feature in Tor . . . to prevent someone from learning the Tor Browser user's true IP address*." *United States v. Wheeler*, No. 1:15-CR-390 (N.D. Ga. Aug. 21, 2017) (emphasis added). He later testified:

> So the Playpen website was a child pornography website that existed within the Tor network running as a Tor hidden service. . . *because it's running as a Tor hidden service*, even though we now have control of the website, *we still don't know who the users are. People can still access the website but we can't see their real IP address. So that's what the NIT does*. . . [W]hen you access the internet through Tor, your real IP address is invisible to the destination. *So what the NIT does is it forces the computer to communicate outside of the Tor network over the regular internet. So when that happens, we can see the defendant's real IP address.*

United States v. Stamper, Case No. 1:15cr109 (S.D. Ohio Mar. 9, 2018) (ECF No. 94 at 69, 75-76) (emphasis added).

B. ARGUMENT

1. There is no process for [redacted]

What FBI Agents have previously stated under oath is substantively [redacted]

[redacted]

[redacted] Ex. 11 (Third Declaration of Dr. Matthew Miller) at 1.

[redacted]

[40] Dr. Miller has previously been qualified as an expert in numerous previous cases that involved child pornography investigations on the Tor network, and the defense is not aware of any instance where the Government objected to Dr. Miller's expertise.

[redacted]

2. **The Special Agent was not aware of any method that could** [redacted]

[redacted]

3. **The Special Agent should have known** [redacted]

[redacted]

[redacted]

[redacted] *United States v. Darby*, 190 F. Supp. 3d 520, 530 (E.D. Va. 2016), *aff'd*, 721 F. App'x 304 (4th Cir. 2018) (deployment of a NIT that obtains data from a person's computer is a search and seizure under the Fourth Amendment).

Given intelligence-sharing agreements between [redacted]

[41] Intelligence and Security Committee of Parliament, Parliament of the United Kingdom, *Privacy and Security: A modern and transparent legal framework* 90-91 (March 2015) (describing how the U.K. shares information with overseas partners, including with members of the Five-Eyes network, which includes the U.S.), available from https://isc.independent.gov.uk/committee-reports/special-reports.

[redacted] *it is precisely why the Framers enacted the Fourth Amendment in the first place*. *Riley v. California*, 573 U.S. 373, 403 (2014) (the Fourth Amendment was meant to protect against "the reviled 'general warrants' and 'writs of assistance' of the colonial era, which allowed British officers to rummage through homes in an unrestrained search for evidence of criminal activity").

The Fourth Amendment's prohibition against unreasonable searches and seizures required the Government [redacted] While something "a person knowingly exposes to the public" is not constitutionally protected, something a person "seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected." *Katz v. United States*, 389 U.S. 347, 351 (1967). People have a reasonable expectation of privacy when using the Tor network because "only the IP address of the last relay computer . . . as opposed to the Tor user's actual IP address, appears on that website's IP address log," and furthermore, "the content of a Tor user's communications are encrypted while the communication passes through the Tor network." Ex. 5 (Affidavit) at ¶ 11; *see also* Ex. 9 (Declaration of Dr. Matthew Miller); Ex. 12 (Fourth Declaration of Dr. Matthew Miller); Ex. 16 (Declaration of Richard Clayton). Even though the Tor Project has

a publicly available webpage that cautions "that the use of the Tor network does not render a user's communication totally anonymous," Ex. 5 (Affidavit) at ¶ 12, [redacted]

V. ALL FRUITS OF THE ILLEGAL SEARCH MUST BE SUPPRESSED.

All tainted fruits, including tangible evidence, electronic evidence, and statements Mr. Sanders made to law enforcement, should be suppressed. The FBI found the tangible evidence, obtained forensic electronic information, and obtained Mr. Sanders's statements by exploiting the illegally obtained search warrant, including by questioning him in his home. Because his statements are clearly the fruit of the poisonous tree, they must also be suppressed. *Wong Sun v. United States*, 371 U.S. 471, 485 (1963) ("verbal evidence which derives so immediately from an unlawful entry and an unauthorized arrest as the officers' action in the present case is no less the 'fruit' of official illegality than the more common tangible fruits of the unwarranted intrusion."); *United States v. Saafir*, 754 F.3d 262, 267 (4th Cir. 2014) (suppressing statements that were fruit of officer's false assertion of authority to search vehicle); *United States v. Watson*, 703 F.3d 684, 697 (4th Cir. 2013) (suppressing statement seized as fruit of unlawful arrest); *United States v. Seidman*, 156 F.3d 542, 548 (4th Cir. 1998) ("If the Government has committed a constitutional violation, however, evidence obtained as a result of the violation cannot be used unless the connection between the unlawful conduct and the acquisition of the evidence has become so attenuated as to dissipate the taint."); *United States v. Brown*, 401 F.3d 588, 592 (4th Cir. 2005)

("Evidence gathered as fruit of an unreasonable search or seizure is generally inadmissible against a defendant."); *see also New York v. Harris*, 495 U.S. 14, 20 (1990) ("The warrant requirement for an arrest in the home is imposed to protect the home, and anything incriminating the police gathered from arresting Harris in his home, rather than elsewhere, has been excluded, as it should have been; the purpose of the rule has thereby been vindicated.").

CONCLUSION

Because the warrant issued in this case was based on a single, uncorroborated hearsay allegation, [redacted], the warrant was not supported by probable cause. Furthermore, because the warrant was based on materially false statements and omissions, and because *even without correcting the Affidavit* it was "so lacking in indicia of probable cause as to render official belief in its existence entirely unreasonable," *United States v. Leon*, 468 U.S. 897, 932 (1984), the *Leon* good faith exception does not apply. As a result, all evidence derived from the illegal search of the Sanders's family home, the illegal interrogation of Mr. Sanders and his parents, and the illegal forensic examinations of any tangible evidence should be suppressed as fruit of the poisonous tree.

Respectfully submitted,

/s/ Jonathan Jeffress

Jonathan Jeffress (#42884)
Emily Voshell (#92997)
Jade Chong-Smith (admitted *pro hac vice*)
KaiserDillon PLLC
1099 Fourteenth St., N.W.; 8th Floor—West
Washington, D.C. 20005
Telephone: (202) 683-6150
Facsimile: (202) 280-1034
Email: jjeffress@kaiserdillon.com
Email: evoshell@kaiserdillon.com

Email: jchong-smith@kaiserdillon.com

Counsel for Defendant Zackary Ellis Sanders

CERTIFICATE OF SERVICE

I hereby certify that on this 27th day of August 2020, the foregoing was served electronically on the counsel of record through the U.S. District Court for the Eastern District of Virginia Electronic Document Filing System (ECF) and the document is available on the ECF system.

/s/ Emily Voshell
Emily Voshell

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
Alexandria Division

UNITED STATES OF AMERICA, Plaintiff, v. ZACKARY ELLIS SANDERS, Defendant.	Case No. 1:20-cr-00143 The Honorable Judge Ellis

[PROPOSED] ORDER

This matter having come before the Court on Mr. Sanders's Motion to Suppress, and have having reviewed the Government's Opposition thereto, it is, for good cause shown, **ORDERED** that the Motion to Suppress is **GRANTED**.

It is so ORDERED.

_____

THE HONORABLE T.S. ELLIS

Date: _____

Alexandria, Virginia